

Gen Docket No. 09-3

Gregory Intoccia

Subject: FW: Workshop
Attachments: FCC Questions.docx

FILED/ACCEPTED

SEP 30 2009

Federal Communications Commission
Office of the Secretary

From: Rich D. Pethia <rdp@cert.org>
To: Joy Ragsdale
Cc: Jennifer Manner
Sent: Fri Oct 30 10:28:00 2009
Subject: RE: FCC Cyber Security Workshop Follow-up

Joy

Attached, please find my responses to the questions you sent on October 9th. I would be happy to discuss these responses or any other issues should you have further questions.

Rich Pethia
Director, CERT Program
Software Engineering Institute, Carnegie Mellon University
412-268-7739

From: Joy Ragsdale [mailto:Joy.Ragsdale@fcc.gov]
Sent: Friday, October 09, 2009 6:02 PM
To: Rich D. Pethia
Cc: Jennifer Manner
Subject: FCC Cyber Security Workshop Follow-up

Mr. Pethia,

In order to ensure we have a more complete record, we would appreciate your comments in response to the attached questions by November 1, 2009.

Thank you

Joy M. Ragsdale, Attorney
FCC, Public Safety & Homeland Security
Policy Division
w) 202-418-1697

*** Non-Public: For Internal Use Only ***

No. of Copies rec'd 2
List ABCDE

10/30/2009

Questions

1. What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are their policies that the U.S. government should consider in the broadband plan to encourage this?
 - Network providers have a responsibility to insure the reliable operation of the network (i.e. insure that the bits keep moving and that they all get to where they are supposed to go in a reasonable period of time). Policies that allow users to seek damages from their immediate and upstream service providers in cases of significant service disruption should go a long way in encouraging the right kind of behavior
2. With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security focused agencies, and competitive service providers?
 - Questions 2, 3 and 4 cannot be answered in any meaningful way until another question is answered:
 - What are the organizations that receive the reports going to do with the information?
 - What actions will they take?
 - In what timeframes will those actions be taken?Discussing information sharing in the abstract has little to no value. The FCC and other agencies need to first define what roles they want to play with respect to security improvement, what structures they will put in place to perform those roles, and then what information they will need to support that activity. If service providers see value in those activities, there will be a basis for a discussion on the details of the data flow.
3. Should there be a uniform or baseline definition of a “cyber security incident” that mandates when service providers report to their customers, the FCC, other government or security focused agencies and competitive service providers a security incident that may be global affecting?
 - See response to 2
4. Should there be a mandatory threshold of affected systems or networks by cyber incidents at which providers must report information to the FCC and other government agencies such as US-CERT and the National Coordination Center (NCC)?
 - See response to 2
5. Should US-CERT, the NCC and any other government-supported entity that receives such information, adhere to confidentiality agreements with commercial providers to allay concerns about the disclosure of competitive market data and proprietary information?
 - Two points here:
 - Questions 2 through 5 all imply a one-way flow of information – from the service provider to some other organization(s). Thought needs to be given to what information will be given TO the service providers. The DoD’s program

that supports the Defense Industrial Base, operated through the Defense Cyber Crime Center, is a working model that will give the FCC insight into one way of bringing about security improvement across a broad set of organizations

- Any information sharing should be governed by a documented set of rules that lay out the details of information sharing in both directions. For each type of data to be shared, who is expected to generate it, when, under what circumstances, who gets it, what will they do with it, what pieces of it (if any) can they share with others.
6. Currently, there are many private and public sector agencies that offer and encourage the adoption of security best practices. How can the FCC or other government-supported entities serve as a repository for centralizing these best practices? What are some ways the government can incent industry to promote the increased use of integrity check and authentication systems?
- I don't know that we need "repositories for centralizing best practices", but would encourage that FCC and other government entities to become "catalysts for raising awareness and understanding and promoting best practices". Activities to sponsor would include:
 - Industry conferences where practitioners are invited to present on the practices they use and their effectiveness
 - On-line discussion forums that focus on security problems and mitigation methods
 - Executive forums that encourage senior management involvement in the implementation of security policies and practices
7. What metrics, resources, or tools can be used to measure whether an organization can sustain its security practices in times of crisis?
- The one example that I know of is the work we've done at CERT. The cornerstone of our research is the development of the CERT * Resiliency Management Model. The model is the foundation for a process improvement approach to security and business continuity. It establishes an organization's resiliency management process: a collection of essential capabilities that an organization performs to ensure that its important assets—people, information, technology, and facilities—stay productive in supporting business processes and services. The model serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security and business continuity activities and takes on a process improvement mindset that helps to keep these activities productive in the long run and in times of crisis.
8. How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing any such vulnerabilities and, if not, what can be done to better address these concerns?

- Over the past 15 years, there have been a number of reports from credible sources regarding counterfeit hardware products as well as software viruses and Trojan horses implanted in copies of software being distributed over the Internet. A recent survey of a group of companies with good reputations for producing secure software shows that these companies use good practices for internal code development, but have very few practices for managing supply-chain risks (BSIMM <http://www.bsi-mm.com/>). This is not that surprising given that these organizations' secure software initiatives are only a few years old. The risks associated with complicated supply chains, are also evident in contracted development and integration. Does an integrator have sufficient knowledge of the risks associated with product features or of the operating assumptions so that the integration of software from multiple sources does not create a vulnerability? The answer is often "no". The integration issues demonstrate the limits of our current practices. All of the participants in the BSIMM survey acknowledged the value of architectural analysis in identifying and resolving vulnerabilities, but none of them did it regularly. The current architectural analysis methods are too difficult to do and require a very experienced staff. The area of supply chain risk management should be viewed as one that still has many open research questions and few proven practices.
9. Several panelists expressed concern that there is a lack of skilled and trained staff available to respond to and resolve security breaches or cyber security attacks. Is this a temporary anomaly, or a long-term deficiency that needs attention? How can federally-funded grant programs assist state agencies, local community, and technical colleges offer degrees or webinar courses on cyber security?
- I believe the shortage of skilled staff is a serious problem now and one that will be with us for some time. In my interactions with government and industry organizations, I frequently see security management/response groups that, while well intended, do not have the comprehensive set of skills needed for successful security work. As the nation becomes increasingly dependent on our information infrastructures and as these infrastructures expand into new areas in new ways (e.g. the evolving Smart Grid), the demand for people with these skills will be even greater. The current NSA and NSF scholarship for service programs (providing fully paid tuition for degree programs in return for matching years of service within DoD or other government agencies) serve as good models of successful programs. These programs not only produce students with the needed skills, but also encourage universities to develop the curriculum and capacity needed to educate the workforce over time.
10. What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may gain access to this information using keyloggers, IP masking or other virtual means to access the end users data?
- ISPs are in a good place to inform their users of the risks, to inform them of ways to combat the risk, and to offer security services and tools that help users protect their systems (e.g. anti-virus/spyware software, anti-spam filters, etc).

11. Would it be possible to implement hashing, 256 or 512 Bit encryption, sha 64+1 RSA Token Authentication to ensure the protection of end users data?

- While possible, I'm skeptical about the benefit. Encryption helps data security as long as it is done from end to end, including the systems at the end points. Protecting users' data in transit provides little benefit unless the users take steps to protect the data that is stored in their machines. Also, there are many simple, affordable ways for users to obtain this kind of protection. As in question 10 above, ISPs could inform users of the risks and provide guidance on the steps needed from effective risk management.



Federal Communications Commission
Washington, D.C. 20554

October 9, 2009

Richard Pethia
Director, CERT
Carnegie Mellon University
SEI-CERT
4500 Fifth Avenue
Pittsburg, PA 15213

Re: National Broadband Plan Proceeding, Docket No. 09-51

Dear Mr. Pethia:

Thank you, very much for your participation in the FCC's October 2, 2009 Cyber Security Workshop. The Workshop was very enlightening and provided important information that will be considered in developing a National Broadband Plan.

As a follow-up to the workshop and in order to ensure we have a complete record, we would appreciate it if you could provide your comments in response to the following questions by November 1, 2009. Of course, your answers will be made part of the public record for the Broadband Plan proceeding.

Questions

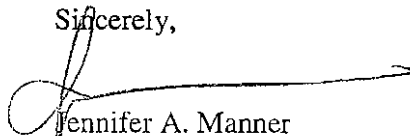
- What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are there policies that the U.S. government should consider in the broadband plan to encourage this?
- With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?
- Should there be a uniform or baseline definition of a "cyber security incident" that mandates when service providers report to their customers, the FCC, other government or security-focused agencies, and competitive service providers a security incident that may be global affecting?
- Should there be a mandatory threshold of affected systems or networks by cyber incidents at which providers must report information to the FCC and other government agencies such as US-CERT and the National Coordination Center (NCC)?

- Should US-CERT, the NCC and any other government-supported entity that receives such information, adhere to confidentiality agreements with commercial providers to allay concerns about the disclosure of competitive market data and proprietary information?
- Currently, there are many private and public sector agencies that offer and encourage the adoption of security best practices. How can the FCC or other government-supported entities serve as a repository for centralizing these different best practices? What are some ways that government can incent industry to promote the increased use of integrity check and authentication systems?
- What metrics, resources or tools can be used to measure whether an organization can sustain its security practices in times of crisis?
- How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing any such vulnerabilities and, if not, what can be done to better address these concerns?
- Several panelists expressed concern that there is a lack of skilled and trained staff available to respond to and resolve security breaches or cyber security attacks. Is this a temporary anomaly, or a long-term deficiency that needs attention? How can federally-funded grant programs assist state agencies, local community and technical colleges offer degrees or webinar courses on cyber security?
- What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may gain access to this information using keyloggers, IP masking or other virtual means to access the end users data?
- Would it be possible to implement hashing, 256 or 512 Bit encryption, sha 64+1, RSA Token Authentication to ensure the protection of the end users data?

Richard Pethia
October 9, 2009
Page 3

Thank you once again. Your contribution will help us shape a bold and innovative vision for how we can develop initiatives to strengthen our nation's broadband networks and protect them from potentially damaging and global affecting cyber attacks. If you have any questions or comments please feel free to contact me at (202) 418-3619 at your convenience.

Sincerely,

A handwritten signature in dark ink, appearing to read "Jennifer A. Manner", with a long horizontal flourish extending to the right.

Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Jennifer.Manner@fcc.gov